UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/725,272	11/29/2000	Hideki Imai	5-030US	8854

7590 06/17/2004

McGinn & Gibb, PLLC
Suite 200
8321 Old Courthouse Road
Vienna, VA 22182-3817

EXAMINER	
NGUYEN, MINH DIEU T	
ART UNIT	**PAPER NUMBER**
2137	2

DATE MAILED: 06/17/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/725,272	IMAI ET AL.	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-82* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *See Continuation Sheet* is/are rejected.

7)☒ Claim(s) *14-16,25,26,32-34,41,44,47,50,53,56,59,68,71,74,77 and 80* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Continuation of Disposition of Claims: Claims rejected are 1-13,17-24,27-31,35-40,42,43,45-46,48-49,51-52,54-55,57-58,60-70,72-73,75-76,78-79, and 81-82.

DETAILED ACTION

1. Claims 1-82 are pending.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 1-12, 17-22, 42-43, 51-58 and 60-64 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a) Claims 1, 5 and 9 recite the limitation "the signer's identity", "the identification code", "the validity", "the signer's identification code" on page 24. There is insufficient antecedent basis for these limitations in the claim.

b) Claims 17-18 recite the limitation "the signer's identification code" on page 31. There is insufficient antecedent basis for this limitation in the claim.

c) Claim 20 recites the limitation "the verifier" on page 32. There is insufficient antecedent basis for this limitation in the claim.

d) Claim 23 recites the limitation "the steps", "the signer's identity", "the signer's identification code" on pages 33-34. There is insufficient antecedent basis for these limitations in the claim.

e) Claim 31 recites the limitation "the verifier's verification-key", "the signer's identification code", "the validity" on pages 37-38. There is insufficient antecedent basis for these limitations in the claim.

f) Claims 53-55 recite the limitation "the number of signers" on page 43. There is insufficient antecedent basis for this limitation in the claim.

g) Claims 56-58 recite the limitation "the number" on page 43. There is insufficient antecedent basis for this limitation in the claim.

4. Claim 27-30, 32-40, 45-46, 48-49, 66-67, 69-70, 72-73, 75-76, 78-79 and 81-82 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential elements, such omission amounting to a gap between the elements. See MPEP § 2172.01.

a) As to claims 27-30, the omitted elements are first, second and third multivariate function.

b) As to claims 32-40, the omitted elements are first and second multivariate function.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. **Claims 1-13, 24 and 31** are rejected under 35 U.S.C. 102(e) as being anticipated by Brown et al., US 6,671,805.

a) **As to claims 1, 5, 9 and 13**, Brown discloses a system and method for document-driven processing of digitally-signed, electronic documents comprising a center computer which reads on a certification authority (col. 22, lines 32-33) wherein the center computer generates and outputs a signing key to be inputted in the first terminal device, and generates and outputs a verification key to be inputted in the second terminal device (col. 22, lines 30-38); a first terminal device which reads on a role identifier (i.e. signer; Fig. 1, element 104) wherein the first terminal device accepts the signing key, generates a digital signature (Fig. 1, element 118) for a digital data (Fig. 1, element 102) to be signed using the signing key (col. 9, lines 21-24), and outputs the digital signature to be inputted in the second terminal device (Fig. 8F); and a second terminal device which reads on a signature verification service (col. 7, lines 20-22) wherein the second terminal device accepts the verification key, signer's identity (col. 8, lines 17-18), identification code of the digital data (Fig. 4A, element 404) and the digital signature, and verifies validity of the digital signature using the verification key, signer's

identification code and identification code of the digital data (col. 22, lines 52-67 – col. 23, lines 1-45).

b) **As to claims 2, 6 and 10**, please see the above addressed claims 1, 5 and 9 for the center computer.

c) **As to claims 3, 7 and 11**, please see the above addressed claims 1, 5 and 9 for the first terminal device.

d) **As to claims 4, 8 and 12**, please see the above addressed claims 1, 5 and 9 for the second terminal device. Brown also discloses the step of outputting the result of verifying the validity of the digital signature, namely, acceptable as valid or not (Fig. 8F, elements 876 Y/N).

e) **As to claim 24**, Brown discloses a first terminal device which reads on a role identifier (i.e. signer; Fig. 1, element 104) comprising an accepting means for accepting a signer's signing key; a first input device inputting the signer's signing key (col. 8, lines 17-21); a second input device inputting an identification code of a digital data (col. 10, lines 18-19); a generating means for generating a digital signature (Fig. 1, element 118), and an output device outputting the digital signature generated by the generating means (Fig. 8F).

f) **As to claim 31**, Brown discloses a second terminal device which reads on a signature verification service (col. 7, lines 20-22) comprising a first accepting means for accepting a verification key; a first input device inputting the verifier's verification key (col. 22, lines 34-36); a second accepting means for accepting a signer's identity (col. 8, lines 17-18); a second input device inputting the signer's identification code; a third accepting means for an identification code of a digital data (Fig. 4A, element 404); a third input device inputting the identification code of the digital data; a fourth accepting means for accepting a digital signature; a fourth input device inputting the digital signature(Fig. 8F, element 862); a verifying means for verifying the validity of the digital signature using the verification key; the signer's identification code and the identification code of the digital data (col. 22, lines 52-67 – col. 23, lines 1-45); an output device outputting the result of verifying the validity of the digital signature, namely, acceptable as valid or not (Fig. 8F, elements 876 Y/N).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claims 62-65** are rejected under 35 U.S.C. 103(a) as being obvious over Brown et al., US 6,671,805 in view of Fischer et al., US 2001/0005823.

Brown discloses the identification code of a digital data, however he fails to teach the id code is a compressed data.

Fischer discloses the identification code of a digital data is a compressed data (page 1, paragraph 0006).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of compression format, as Fischer teaches, in the system of Brown so as to get more effective disk storage.

Allowable Subject Matter

9. Claims **14-16, 25-26, 32-34, 41, 44, 47, 50, 53, 56, 59, 68, 71, 74, 77, 80** are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

10. Claims **17-23, 27-30, 35-40, 42-43, 45-46, 48-49, 51-52, 54-55, 57-58, 60-61, 66-67, 69-70, 72-73, 75-76, 78-79 and 81-82** would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, second paragraph, set forth in this Office action.

The prior arts of Brown et al., Fischer et al., Herzberg et al. and Hoffstein et al. do not disclose the method of claims 17, 20, 23, 27, 29, 35 and 38 where signing key, verification key and digital signature are established. In particular, a verification key is established by outputting a random number and a third multivariate function wherein the third multivariate function obtained by substituting the random number into a second variable of the first multivariate function; a digital signature is established by outputting a fourth multivariate function wherein the fourth multivariate function obtained by substituting the identification code of the digital data into the third variable of the second multivariate function; a first evaluation value is established by substituting the random number into the second variable of the fourth multivariate function and a second evaluation value by substituting the signer's identification code and the identification code of the digital data into the first and third variables of the third multivariate function, respectively, and the digital signature is accepted as valid if both the first and second evaluation values equal, otherwise the digital signature is rejected as invalid.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure

a) US 6,154,841 to Oishi discloses digital signature method and communication system.

b) US 6,446,206 to Feldbaum discloses method and system for access control of a message queue.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 703-305-9727. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn
6/7/04

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100